

# FortiAuthenticator - Certificate Based SSL VPN Solution Guide

**VERSION 1.0**

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



09/10/2015

FortiAuthenticator 4.0 - Certificate Based SSL VPN Solution Guide

23-330-264235-20150901

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Software Versions	5
<b>FortiAuthenticator Certificate Based SSL VPN Guide</b>	<b>6</b>
Introduction	6
Topology	6
FortiAuthenticator Root Certificate	7
FortiAuthenticator User Certificate	8
FortiAuthenticator Directory Services Configuration	13
FortiGate Certificate Configuration	15
FortiGate RADIUS Client Configuration	15
FortiGate SSL-VPN Configuration	17
Testing, Logging and Monitoring	20
Additional Considerations - Certificate Checking	24
Added Benefits	24

## Change Log

Date	Change Description
2013-10-23	Initial revision

# Introduction

This document provides a configuration guide for setting up certificate based SSL-VPNs using FortiGate and FortiAuthenticator. The guide provides a step by step walkthrough on both the FortiAuthenticator and the FortiGate, however, for a detailed understanding on PKI and certificate authentication further reading is required, as the objective of this guide is to provide a configuration walkthrough.

## Software Versions

The configuration discussed in this document was tested on the following firmware versions:

- FortiAuthenticator 3.0
- FortiOS 5.0 GA Patch Release 4

# FortiAuthenticator Certificate Based SSL VPN Guide

## Introduction

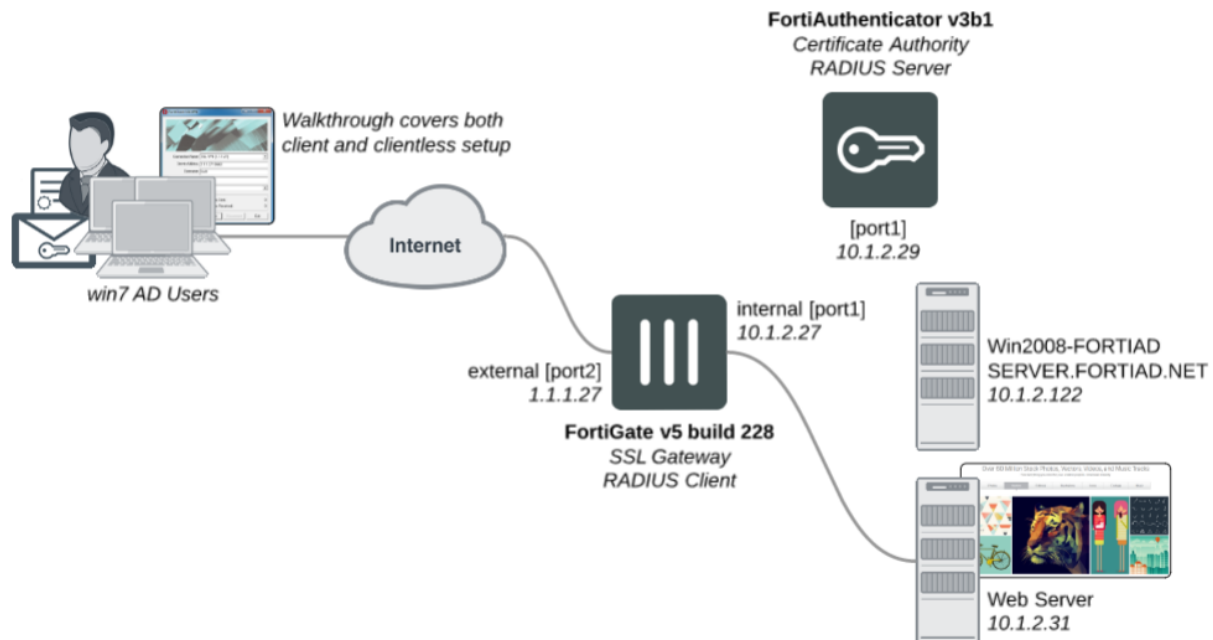
The purpose of this document is to provide a configuration guide on how to setup certificate based SSL-VPNs, using FortiGate and FortiAuthenticator. The guide covers various subject areas such as PKI and VPNs, further reading is required for a detailed understanding on the theory of such topics, the intention of this document is to provide a concise configuration guide which will allow for the successful configuration of certificate based VPNs.

The guide will step through the FortiAuthenticator configuration before moving on the FortiGate, before testing the setup. All the topology components are using factory default settings, except for the IP configuration.



Before commencing the configuration, please ensure that the date and time are correctly configured and synchronized across all of the topology elements.

## Topology



## FortiAuthenticator Root Certificate

To commence the certificate setup on the FortiAuthenticator, a Certificate Authority root certificate has to be created (the FortiAuthenticator is the Certificate Authority in this configuration).

Under *Certificate Management > Certificate Authorities > Local CAs* click *Create New*.

Complete the relevant certificate, example below and OK the changes.

Create New Local CA Certificate

Certificate ID: facv3\_b1

Certificate Authority Type

**Certificate type:**
☒ Root CA certificate
 ☐ Intermediate CA certificate
 ☐ Intermediate CA certificate signing request (CSR)

Subject Information

**Subject input method:**
☐ Fully distinguished name
 ☒ Field-by-field

**Name (CN):** FortiAuthenticator

Department (OU):

Company (O):

City (L):

State/Province (ST):

Country (C): 

▼

E-mail address:

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

Additional Options

**Validity period:**
☒ Set length of time
 ☐ Set an expiry date

3650 days

**Key type:** RSA

**Key size:** 2048 Bits ▼

**Hash algorithm:** SHA-1 ▼

OK

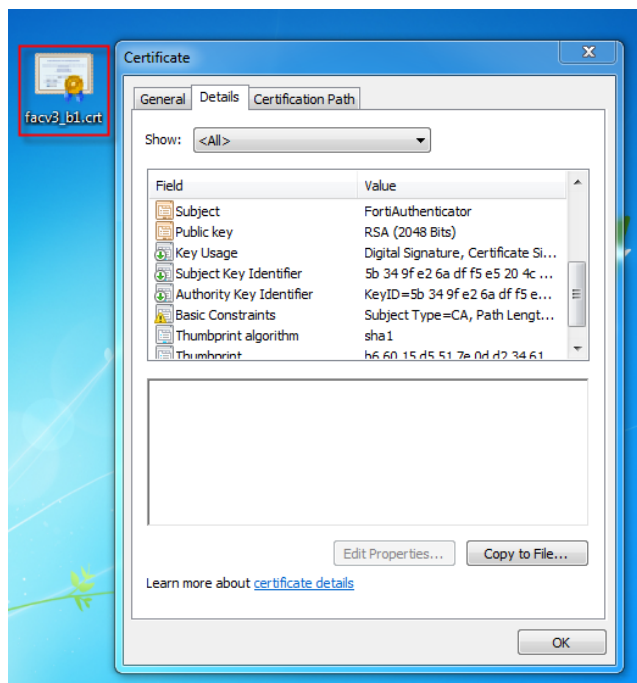
Cancel

Once the certificate has been created, select the certificate and then click on *Export*.

✓ Successfully added local CA certificate "facv3\_b1 | CN=FortiAuthenticator".

	Certificate ID	Subject	Issuer	Status	CA Type
✓	facv3_b1	CN=FortiAuthenticator	CN=FortiAuthenticator	Active	Root CA

Save the certificate to the desktop (or appropriate folder). Once the certificate is saved, it should be possible to double click on the certificate to view the details, see below.



## FortiAuthenticator User Certificate

The next certificate based task is to create the user certificate. Within the FortiAuthenticator interface, go to *Certificate Management > End Entities > Users* and click on *Create New*. Then complete the relevant user certificate fields and click on *OK*, example below.



**Create New User Certificate**

**Certificate ID:**

**Certificate Signing Options**

**Issuer:** ☒ Local CA ☐ Third-party CA

**Local User (Optional):**

**Certificate authority:**

**Subject Information**

**Subject input method:** ☐ Fully distinguished name ☒ Field-by-field

**Name (CN):**

**Department (OU):**

**Company (O):**

**City (L):**

**State/Province (ST):**

**Country (C):**

**E-mail address:**

**Subject Alternative Name**

☐ Email:

☐ User Principal Name (UPN):

**Additional Options**

**Validity period:** ☒ Set length of time ☐ Set an expiry date

days

**Key type:** RSA

**Key size:**

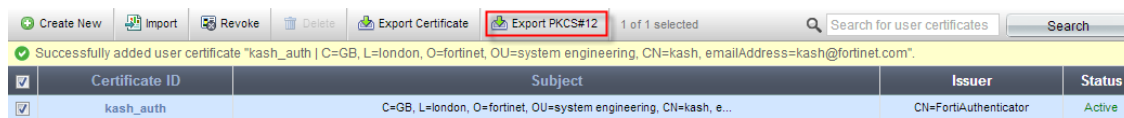
**Hash algorithm:**

**Other Extensions**

☐ Add CRL Distribution Points extension (Location: DNS domain name has not been configured) [Edit DNS name]

☐ Use certificate for Smart Card logon

Once the certificate has been completed and OK'd, then export the certificate with the private key by selecting the certificate and clicking on *Export PKCS12#* button.



Add a *Passphrase* to the certificate being exported and click *OK*.


**Export User Certificate and Key File**

Subject:	C=GB, L=london, O=fortinet, OU=system engineering, CN=kash, emailAddress=kash@fortinet.com
Passphrase:	.....
Confirm Passphrase:	.....

Then download the file to the desktop (or appropriate folder) by clicking *Finish*.

**Download PKCS#12 Certificate File**

Please note that once you click on the download link below, the private key for certificate "C=GB, L=london, O=fortinet, OU=system engineering, CN=kash, emailAddress=kash@fortinet.com" will be removed.

 [Download PKCS#12 file](#)

Click **Finish** to return to the certificate list.

The PKCS12# file should be in the following format on the desktop:



Double click the PKCS12# file, this should then start an automatic import wizard, see below. On the Welcome screen, click *Next*.

**Certificate Import Wizard**



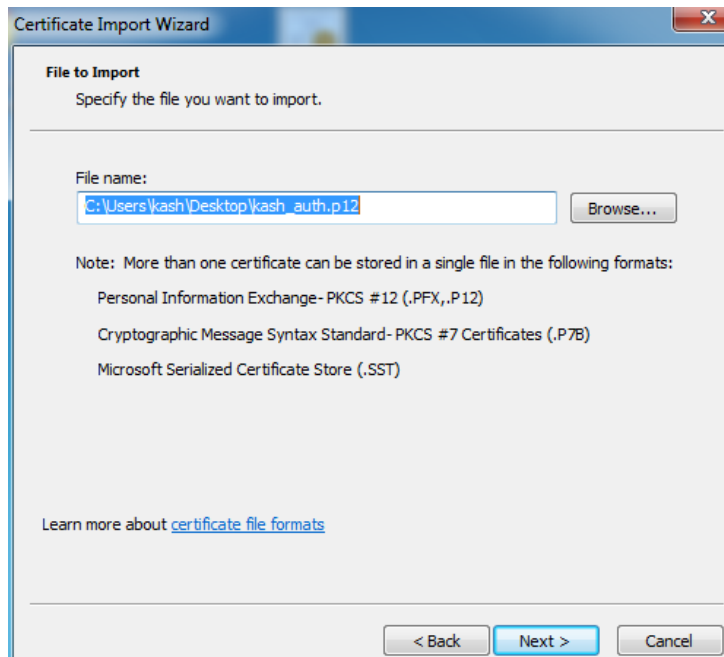
**Welcome to the Certificate Import Wizard**

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

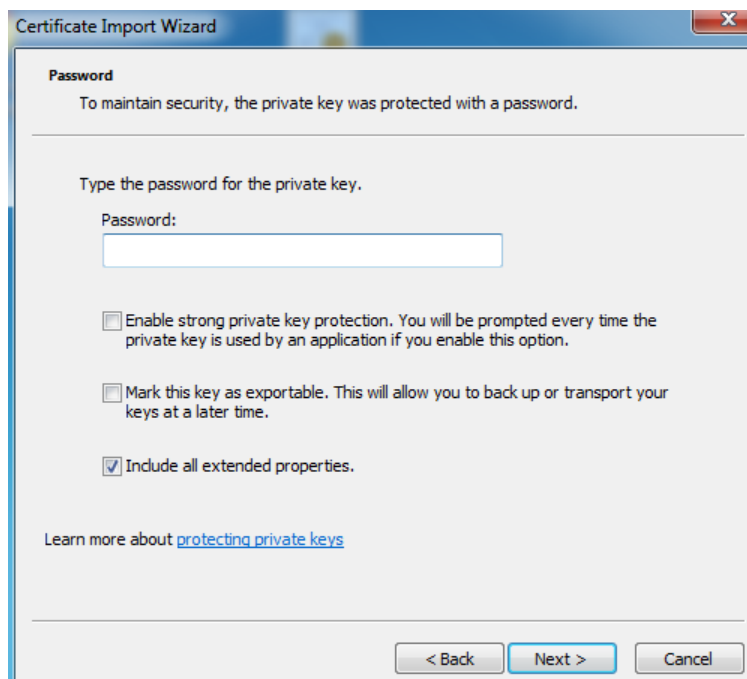
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

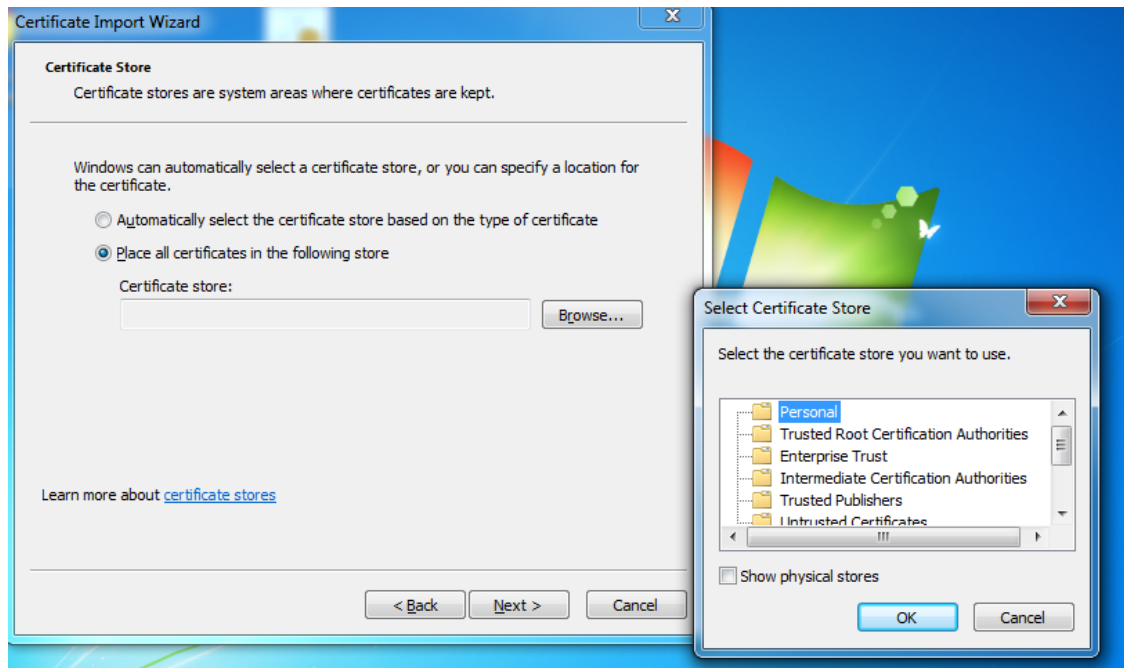
Ensure that the correct PKCS12# file is selected and click *Next*.



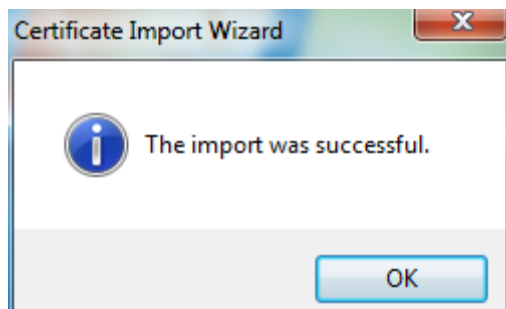
Enter the passphrase used during the export from the FortiAuthenticator and click *Next*.



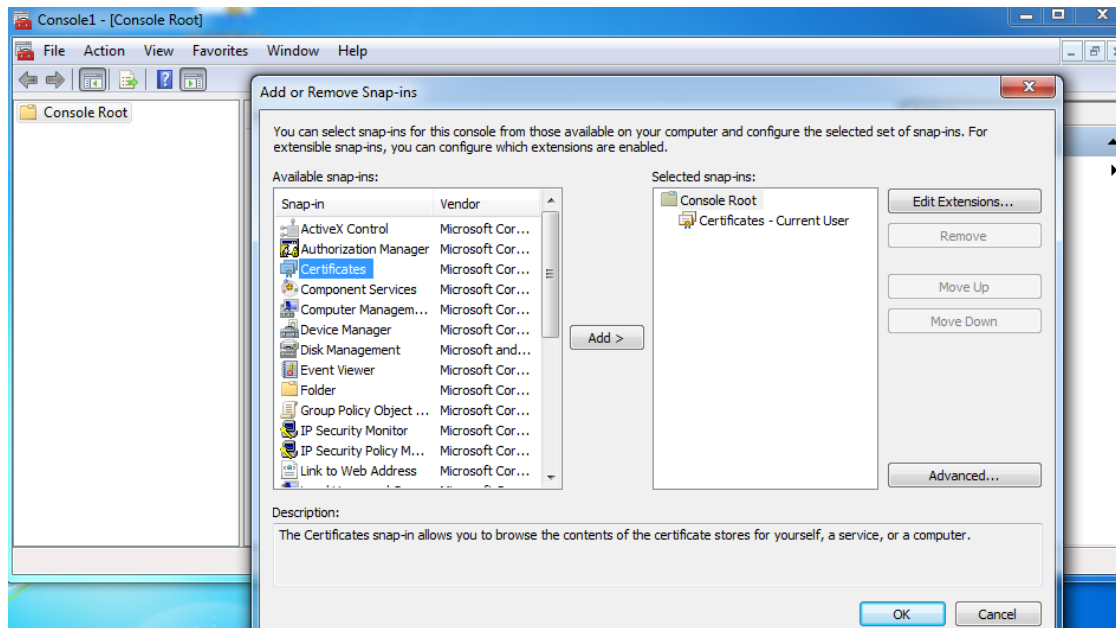
Ensure that the user certificate is being placed in the personal folder and click on *OK*.



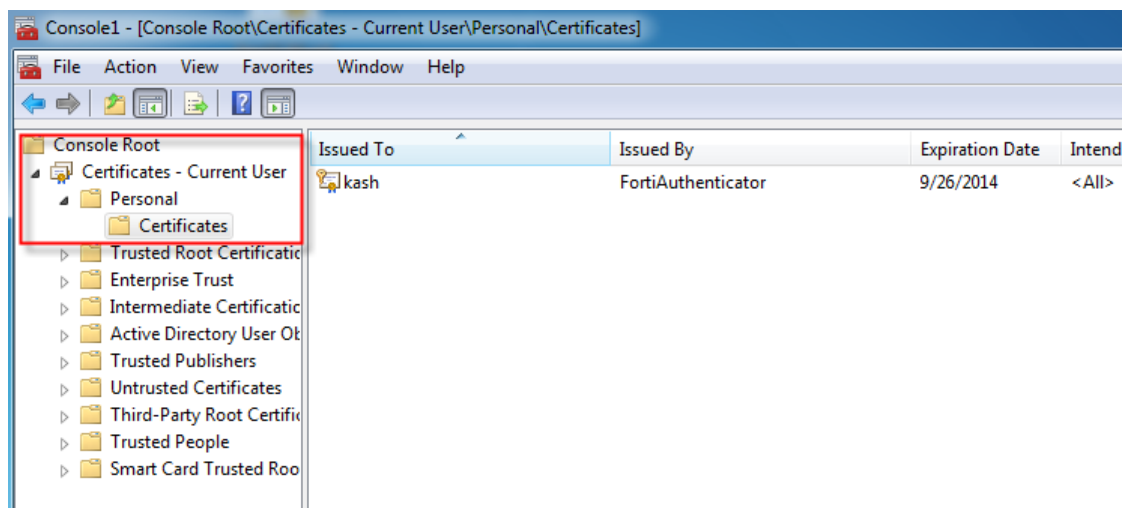
This should complete the user certificate import process and the following prompt should appear:



However, it is important to ensure that the certificate has been imported correctly and into the appropriate certificate store. To confirm the procedure, click on the Windows icon and type *mmc*, then press *Enter*. Then click on *File > Add/Remove Snap-In* and select the *Certificates* snap-in, as shown below, then press *OK*.




In the *Certificates* snap-in, open the *Personal > Certificates* folder. This is where you should find the imported certificate. If this is not the case, do not proceed until the certificate is in place.



This completes the Windows management console tasks, feel free to close the mmc or save the view, it is no longer required in this setup. The certificate tasks on the FortiAuthenticator are now also complete.

## FortiAuthenticator Directory Services Configuration

The following section covers FortiAuthenticator directory integration. To configure integration with a remote AD/LDAP, within the user interface, under *Authentication > Remote Auth. Servers > LDAP*, click on *Create New*, and complete the AD server settings similar to the output below:

Name:	server-2008		
Server name/IP:	10.1.2.122	Port:	389
Base distinguished name:	dc=fortiad,dc=net 		
Bind type:	<input type="radio"/> Simple <input checked="" type="radio"/> Regular		
Username:	cn=administrator,cn=users,dc=fortiad,dc=ne	Password:	.....
User object class:	person		
Username attribute:	sAMAccountName		
Group membership attribute:	memberOf		
<b>Secure Connection</b>			
<input type="checkbox"/> Enable			
<b>Windows Active Directory Domain Authentication</b>			
<input checked="" type="checkbox"/> Enable			
Kerberos realm name:	FORTIAD.NET		
Domain NetBIOS name:	SERVER		
FortiAuthenticator NetBIOS name:	FAC_v3b1		
Administrator username:	administrator		
Administrator password:	.....		

The username and password required do not necessarily have to belong to an administrator; the user only requires enough rights to browse the directory for the purposes of pulling users and groups into the FortiAuthenticator. The *Windows Active Directory Domain Authentication* section does not have to be completed as a requirement for this configuration.

Once the details have been entered, click on the folder icon (next to the *Base Distinguished Name* field) to ensure that you can browse the directory. If the directory is accessible, close the browsing window and click on **OK**.

The next step is to import the user (the one intended for SSL remote access) from the directory to the FortiAuthenticator. The user must be in place on the FortiAuthenticator as in the current version (v3.0), as unknown user authentication is not supported.

In the user interface go to *User Management > Remote Users* and click on *Import*, then select the relevant pre-defined remote LDAP server and click on *Import Users*. From the pop-up window select the relevant user(s) and click on **OK**. The remote user(s) should appear as follows:

<div>  Import            Export Users            Delete            Edit           0 of 1 selected           <div>Search for remote LDAP u</div> </div>		
Username	Remote LDAP server	Admin
kash	server-2008 (10.1.2.122:389)	
1 remote LDAP user		

The final FortiAuthenticator task is to define the FortiGate as a RADIUS client. In the interface, go to *Authentication > RADIUS Service > Clients* and click on *Create New*. Then enter the appropriate details (example below) and click on **OK**.

Edit RADIUS Client	
Name:	FGT-10.1.2.27
Client name/IP:	10.1.2.27
Secret:	••••••••
Description:	
Authentication method:	<input type="radio"/> Enforce two-factor authentication <input type="radio"/> Apply two-factor authentication if available (authenticate any user) <input checked="" type="radio"/> Password-only authentication (exclude users without a password) <input type="radio"/> FortiToken-only authentication (exclude users without a FortiToken)
Authenticate:	<input type="radio"/> All local users <input type="radio"/> Local users from selected groups only (select groups below) <input checked="" type="radio"/> All remote users <input type="radio"/> Remote users from selected groups only (select groups below) <input type="radio"/> All Windows AD users <input type="radio"/> Windows AD users from selected groups only (select groups below)
Remote LDAP server:	server-2008 (10.1.2.122:389) ▼

## FortiGate Certificate Configuration

The next set of tasks will be carried out on the FortiGate. Initially the FortiAuthenticator root certificate needs to be imported into the FortiGate. To do this, within the user interface, go to *System > Certificates > CA Certificates* and then click on *Import*. Click *Local PC* and choose your file, then select the root certificate and click on *OK*.

The imported root CA should look as follows:

<div><div>Delete</div><div>Import</div><div>View Certificate Detail</div><div>Download</div></div>			
<div><div></div></div>	<div>Name</div>	<div>Subject</div>	<div>Re</div>
<div><div></div></div>	<div>CA_Cert_1</div>	<div>CN = FortiAuthenticator</div>	<div><a href="#">0</a></div>
<div><div></div></div>	<div>Fortinet_CA</div>	<div>C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com</div>	<div><a href="#">0</a></div>
<div><div></div></div>	<div>PositiveSSL_CA</div>	<div>C = GB, ST = Greater Manchester, L = Salford, O = Comodo CA Limited, CN = PositiveSSL CA</div>	<div><a href="#">0</a></div>

## FortiGate RADIUS Client Configuration

The FortiGate now needs to be configured as a RADIUS client to the FortiAuthenticator. Within the FortiGate interface, go to *User & Device > Authentication > RADIUS Server* and click on *Create New*. Complete the RADIUS server details, and then test the connection, example below:

The screenshot shows the FortiGate VM64 web interface. The left sidebar has a tree view with 'User & Device' selected, and 'RADIUS Server' is highlighted under the 'User' section. The main panel is titled 'Edit RADIUS Server'. It contains the following fields and options:

- Name:** FortiAuth-Radius-29
- Primary Server Name/IP:** 10.1.2.29
- Primary Server Secret:** A masked field with a 'Test' button next to it.
- Secondary Server Name/IP:** (Empty)
- Secondary Server Secret:** A masked field with a 'Test' button next to it.
- Authentication Scheme:** Radio buttons for 'Use Default Authentication Scheme' (selected) and 'Specify Authentication Protocol'. Below it is a dropdown menu set to 'PAP'.
- NAS IP/Called Station ID:** (Empty)
- Include in every User Group:** A checkbox labeled 'Enable' which is checked.

At the bottom right are 'OK' and 'Cancel' buttons.

Next, a wildcard RADIUS user needs to be created. Go to *User & Device > User > User Definition* and click on *Create New*. Create a wildcard user as shown below. A wildcard user will allow the FortiGate to send all RADIUS authentication requests to the FortiAuthenticator.

The screenshot shows the FortiGate VM64 web interface. The left sidebar has a tree view with 'User & Device' selected, and 'User Definition' is highlighted under the 'User' section. The main panel is titled 'Edit User'. It contains the following fields and options:

- User Name:** A field containing an asterisk (\*) representing a wildcard.
- Disable:** A checkbox which is unchecked.
- Password:** A masked field with a 'Test' button next to it.
- Match user on LDAP server:** A radio button which is unchecked, with a '[Please Select]' dropdown.
- Match user on RADIUS server:** A radio button which is selected, with a dropdown menu set to 'FortiAuth-Radius-29'.
- Match user on TACACS+ server:** A radio button which is unchecked, with a '[Please Select]' dropdown.
- Contact Info:**
  - Email Address:** (Empty)
  - SMS:** Radio buttons for 'FortiGuard Messaging Service' (selected) and 'Custom'. Below it is a 'Phone Number' field.
- Enable Two-factor Authentication:** A checkbox which is unchecked.
- Add this user to groups:** A checkbox which is unchecked.

At the bottom right are 'OK' and 'Cancel' buttons.

The next RADIUS configuration step is to create the RADIUS group on the FortiGate which will host the user(s) for the SSL-VPN. Within the FortiGate go to *User & Device > User > User Group*, click on *Create New*, and create a firewall authentication group that includes the wildcard user and references the FortiAuthenticator, example below:



**Edit User Group**

Name:

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members:

Remote authentication servers

Remote Server	Group Name
FortiAuth-Radius-29	Any

Go back to the wildcard user in *User & Device > User > User Definition* and add the wildcard user to the RADIUS group and OK the changes, example below:

☒ Add this user to groups

☐ Guest-group

☐ dummy-redirect

☐ fortiad\_net-group

☐ radius

☒ radius-auth

## FortiGate SSL-VPN Configuration

The following steps address SSL-VPN creation on the FortiGate. Firstly ensure that there is a valid IP pool in place (under *Firewall Objects > Addresses*), if using an IP tunnel based VPN. To begin the SSL configuration, for both IP tunnel based and browser only VPN, go to *VPN > SSL > Config* and ensure the relevant settings are in place. Also make sure that the *Require Client Certificate* tickbox is selected, as in the example below:

**System**

**Router**

**Policy**

**Firewall Objects**

**Security Profiles**

**VPN**

IPsec

SSL

Portal

**Config**

Monitor

**SSL-VPN Settings**

IP Pools:

---

Server Certificate:

**Require Client Certificate** ☒

Encryption Key Algorithm: ☐ High - AES(128/256 bits) and 3DES

☒ Default - RC4(128 bits) and higher

☐ Low - RC4(64 bits), DES and higher

Idle Timeout:  (seconds)

Login Port:

☐ Allow Endpoint Registration (Tunnel Mode Only)

**Advanced** (DNS and WINS Servers)



Under **VPN > SSL > Portal** create the relevant SSL portal interface based on your VPN type (either IP tunnel or browser only). IP tunnel based VPN is shown in the example below:

**Edit SSL-VPN Portal**

Name:

Portal Message:

Theme:

Page Layout:  

☒ Enable Tunnel Mode

☒ Enable Split Tunneling

IP Pools:

Client Options: ☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

☒ Enable Web Mode

Applications: ☒ HTTP/HTTPS ☐ FTP ☐ RDP ☐ SMB/CIFS  
☐ SSH ☐ TELNET ☐ VNC ☐ PING  
☐ CITRIX ☐ RDP NATIVE ☐ Port Forward

☒ Include Session Info  
☐ Include Connection Tool  
☐ Include FortiClient Download  
☒ Include Bookmarks

[Create New](#) [Edit SSL-VPN Portal](#) [Delete](#)

Name	Type	Location	Description
<b>Intranet (1)</b>			
Intranet Home	HTTP/HTTPS	10.1.2.31	

Within the FortiGate, go to **Policy & Objects > IPv4**, click on **Create New**, then click on VPN setup and create an external interface to internal interface SSL-VPN policy, ensuring that you enable the **SSL client restrictive** tickbox as shown in the example below:

Policy Type: ☐ Firewall ☒ VPN

Incoming Interface:

Remote Address:

Local Interface:

Local Protected Subnet:

☒ **SSL Client Certificate Restrictive**

Cipher Strength:

**Configure SSL-VPN Authentication Rules**

[Create New](#) [Edit](#) [Delete](#)

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
ANY	ALL	always	-		-	DENY

Comments:  0/1023

From within the policy configuration click on **Create New** under the **Configure SSL-VPN Authentication Rules** section and use the preconfigured RADIUS group and the SSL-VPN portal as in the example below. OK the changes and then OK the main policy.

New SSL VPN Authentication Rule ✕

Group(s) radius-auth +

User(s) Click to add...

Schedule always v

SSL-VPN Portal tunnel-access ✕

Action ✓ ACCEPT

**Logging Options**

☐ No Log

☒ Log Security Events

☐ Log all Sessions

**Security Profiles**

OFF AntiVirus

default

OFF Web Filter

default

OFF Application Control

default

OFF IPS

default

OK
Cancel

If the completed SSL policy is selected and edited, the configuration should be as follows:

New Policy

Policy Type ☒ Firewall ☐ VPN

Incoming Interface port2 (external) +

Remote Address all +

Local Interface port1 (internal) +

Local Protected Subnet webserver [10.1.2.31] +

☒ SSL Client Certificate Restrictive

Cipher Strength Any

**Configure SSL-VPN Authentication Rules**

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
radius-auth	ALL	always	-	tunnel-access	<span style="color: blue;">v</span>	✓ ACCEPT
ANY	ALL	always	-			✗ DENY

Comments Write a comment... 0/1023

OK
Cancel

When configuring an IP tunnel SSL-VPN (using the FortiClient), an additional firewall policy is required (configured under *Policy & Objects > IPv4* and then *Create New*). This is to allow incoming connections from the SSL tunnel interface to the internal network. An example of this is as follows:

New Policy

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	ssl.root (sslvpn tunnel interface) <span style="float: right;">+</span>
Source Address	SSL_RANGE_10_1_2_X <span style="float: right;">+</span>
Outgoing Interface	port1 (internal) <span style="float: right;">+</span>
Destination Address	webserver [10.1.2.31] <span style="float: right;">+</span>
Schedule	always <span style="float: right;">v</span>
Service	ALL <span style="float: right;">+</span>
Action	✓ ACCEPT <span style="float: right;">v</span>
<input type="checkbox"/> Enable NAT	

**Logging Options**

- ☐ No Log
- ☒ Log Security Events
- ☐ Log all Sessions

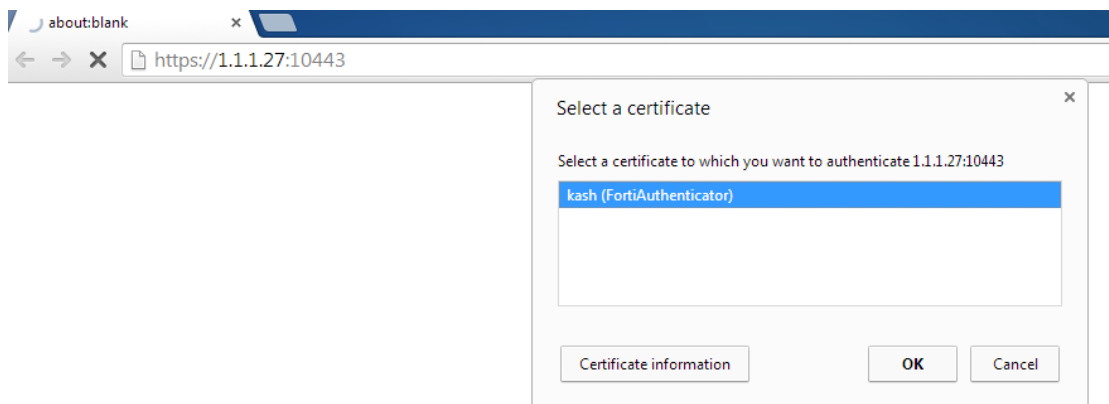
Once you OK the changes, the completed rule should look as follows in the policy section:

▼ ssl.root (sslvpn tunnel interface) - port1 (internal) (2 - 2)						
2	SSL_RANGE_10_1_2_X	webserver [10.1.2.31]	always	ALL		✓ Accept

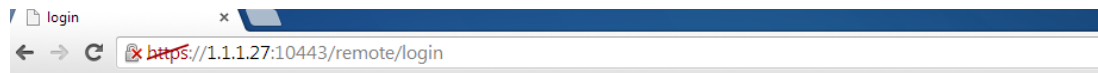
This completes all configuration steps. It is now time to test the VPN.

## Testing, Logging and Monitoring

If the configuration is for a browser only SSL-VPN, then open a browser to the SSL-VPN gateway. Upon connecting to the gateway, the certificate negotiations should begin and the browser should prompt for a valid user certificate to be used for the VPN. Any certificates in the personal certificate store will be listed. See the example below using the Chrome browser:



Upon successful certificate negotiations, a username and password prompt should appear. Even if the certificate negotiations fail, the username and password prompt will still appear, however it will not be possible to successfully authenticate, even if the username and password are valid.

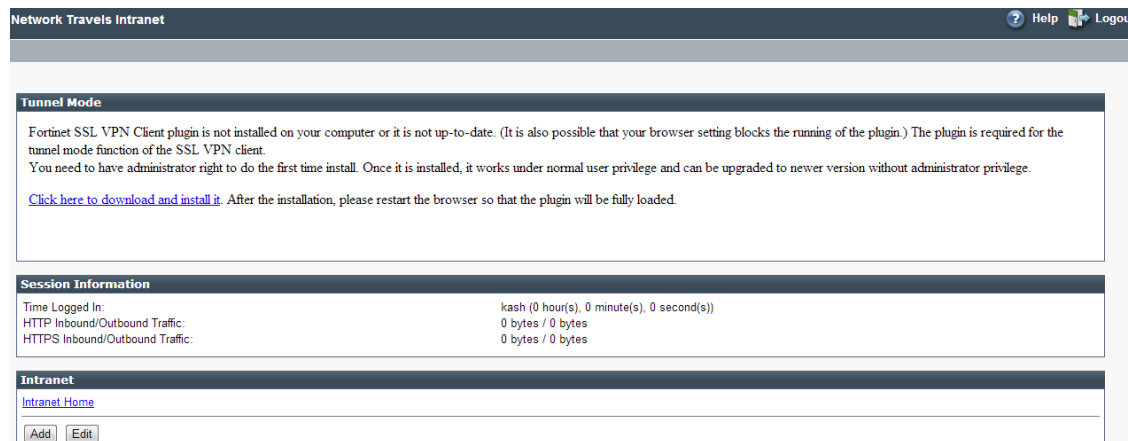


**Please Login**

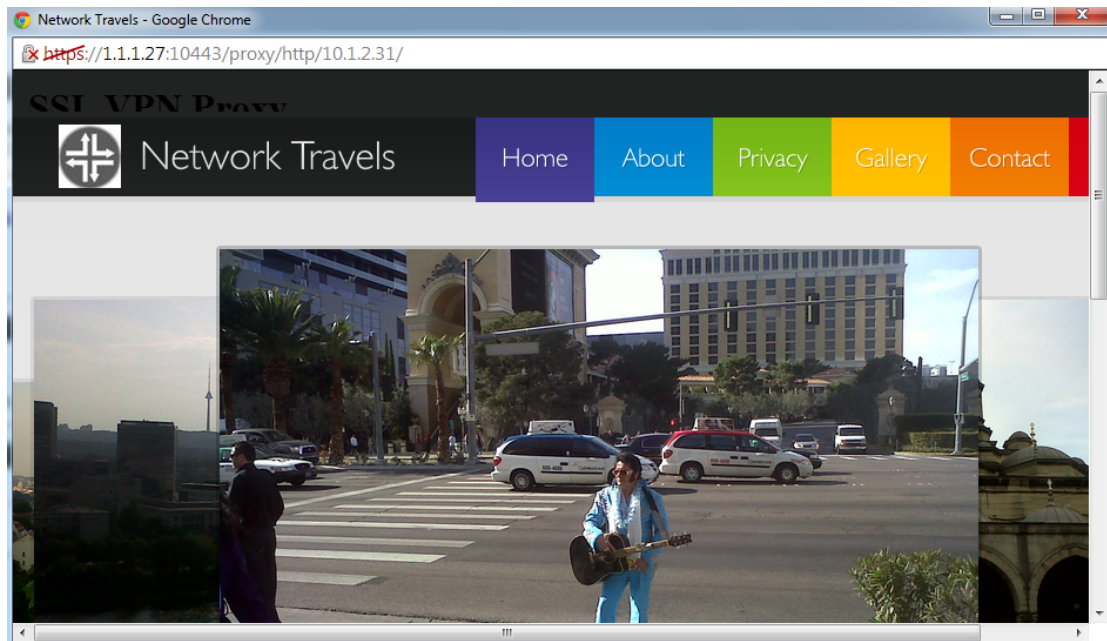
**Name:**

**Password:**

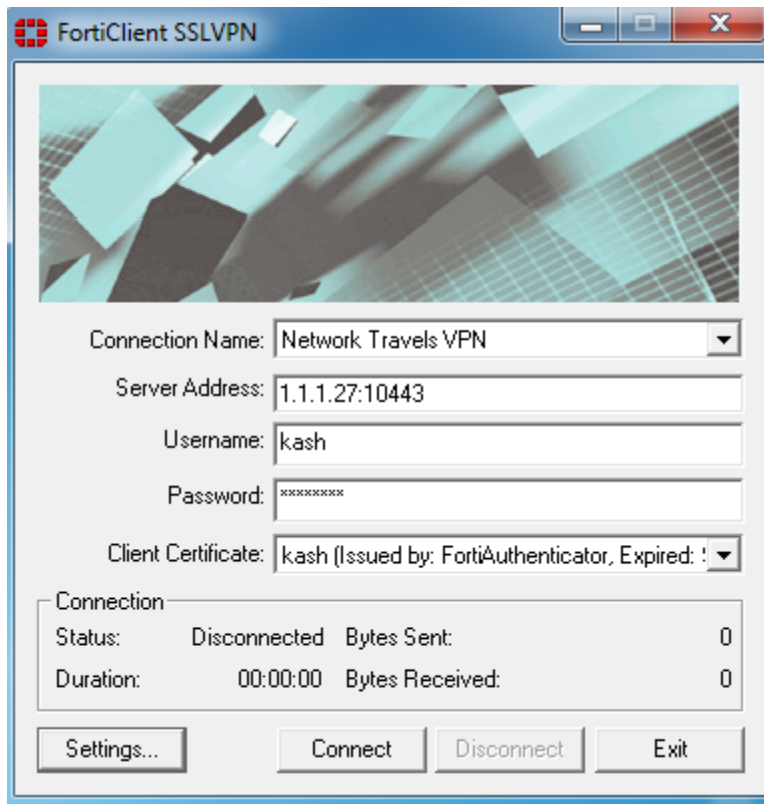
Once the current directory username and password have been entered, the SSL-VPN portal should be available. The example below is of the portal configured earlier in this guide:



Upon clicking on the Intranet homepage, the browser connection is then proxied to the internal web server, as shown in the example below:



If the configuration is based on an IP tunnel configuration, then the FortiClient is required to initiate the connection. The FortiClient should automatically pull the personal certificate from the local certificate store and make it available in the connection settings. See the example below:



Click on *Connect* to initiate the VPN and certificate negotiations. If the certificate negotiations fail, there should be an *-12 error message* prompt and the VPN will not complete. If the certificate settings are valid and the

directory username and password are correct, the VPN should connect and data transfer should begin. To confirm that the client is connected, click on the Windows icon and enter *ipconfig*. The fortissl adapter should be visible with the correct preconfigured address.

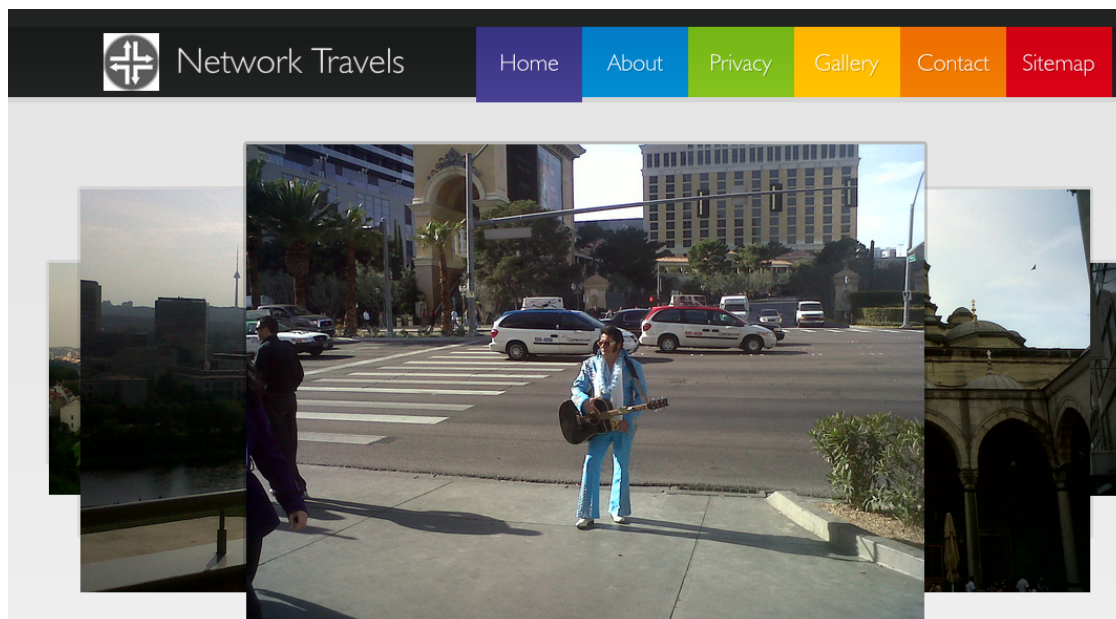
```
C:\Users\kash>ipconfig

Windows IP Configuration

PPP adapter fortissl:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.1.2.151
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . :
```

The client PC should be able to connect to the internal network directly; the image below is of the client browser connecting directly (via the 10.1.2.31 address) to the intranet.



Recent Updates

Aggregating IP Flows

If logging had been enabled on the relevant FortiGate firewall policies, these should also be incrementing their counters and indicating data transfer.

Within the FortiGate, under *VPN > Monitor > SSL-VPN Monitor*, the monitor status should indicate that the client is connected. In the example below, the tunnel IP is also shown as this is a IP tunnel based VPN.

No.	User	Source IP	Begin Time	Description
1	kash	1.1.1.1	Fri Sep 27 08:50:12 2013	
		Subsession		Tunnel IP:10.1.2.151

Within the FortiAuthenticator, under *Logging > Log Access > Logs*, the following entry confirms that the user has successfully authenticated against Active Directory.

306	Fri Sep 27 08:49:49 2013	Information	Event	Authentication	20001	10.1.2.27	Remote LDAP user authentication with no token successful	kash
-----	--------------------------	-------------	-------	----------------	-------	-----------	--	------

This completes and confirms the SSL-VPN client testing.

## Additional Considerations - Certificate Checking

With the above setup, the FortiGate does not check the validity of the received client certificate. This can be achieved through the use of a CRL (Certificate Revocation List) and CDP (CRL Distribution Point). The CRL is a list of certificates the FortiAuthenticator has revoked, and is available to download as a static list. The CDP is in every certificate the FortiAuthenticator issues and provides a link for the CRL. OCSP (Online Certificate Status Protocol) is a real-time certificate check with the Certificate Authority. Upon receipt of a certificate, a device can check the validity of the certificate from the issuing authority by using OCSP. FortiAuthenticator supports CRLs, CDPs and OCSP.

The dynamic OCSP CRL is accessible via the URL:

`http://<FortiAuthenticator_IP>:2560`

## Added Benefits

- FortiAuthenticator can introduce Certificate Management to an existing FortiGate install base with minimal disruption.
  - With an easy to use interface and rich feature set, customers can increase the security of existing SSL or IPSec VPNs.
- FortiAuthenticator supports SCEP (Simple Certificate Enrolment Protocol), which means users can generate and auto-enroll their certificates, rather than manually creating them.
- Very useful in BYOD and smartphone/tablet scenario's.
- FortiAuthenticator can import users from an existing directory server and associate multiple authentication methods to the user such as FortiTokens, SMS and E-mail.
- Users and Groups can be auto-imported (based on rules) from the directory server.
- Active Directory authenticated users can feed into the FSSO (Fortinet Single Sign-On) framework allowing Identity Based access control across the network.





High Performance Network Security



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.